(19)日本国特許庁（ＪＰ）　(12) 公表特許公報（Ａ）　(11)特許出願公表番号
特表2001－505375
（P2001－505375A）
(43)公表日　平成13年4月17日(2001.4.17)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｈ04Ｌ　9/08		Ｈ04Ｌ　9/00		601C
Ｈ04Ｑ　7/38				601E
		Ｈ04Ｂ　7/26		109R

審査請求　未請求　予備審査請求　有　（全 19 頁）

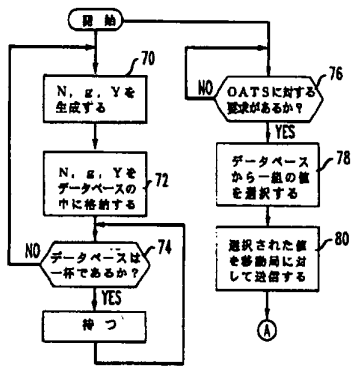
(21)出願番号　特願平10－517588
(86)（22)出願日　平成９年９月29日(1997.9.29)
(85)翻訳文提出日　平成11年４月９日(1999.4.9)
(86)国際出願番号　ＰＣＴ／ＵＳ９７／１７５８５
(87)国際公開番号　ＷＯ９８／１６０３５
(87)国際公開日　平成10年４月16日(1998.4.16)
(31)優先権主張番号　０８／７３１，１０５
(32)優先日　平成８年10月９日(1996.10.9)
(33)優先権主張国　米国（ＵＳ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＢＲ，ＣＡ，ＪＰ，ＭＸ

(71)出願人　エイ・ティ・アンド・ティ・ワイヤーレス・サーヴィスズ・インコーポレーテッド
アメリカ合衆国．98033　ワシントン，カークランド，カロリン　ポイント　5000
(72)発明者　デリー，ブリアン，ケヴィン
アメリカ合衆国．98053　ワシントン，レッドモンド，エヌ．イー．28ストリート　22502
(72)発明者　オーウェンズ，リッスル，デール
アメリカ合衆国　98029　ワシントン，アイサクアー，エス．イー．ツエンティ　フィフス　ウェイ　25712
(74)代理人　弁理士　岡部　正夫　（外10名）

(54)【発明の名称】　改良形暗号化キーの生成

(57)【要約】
一組のディフィー・ヘルマンのデータ暗号化値が、そのデータ　号化値に対する要求の受信に先立って生成される．そのデータ暗号化値は次のデータベースの中に格納される．その生成および格納のステップが繰り返し実行され、データベースの中にデータ暗号化値の格納されたテーブルが作成される．新しいユーザが移動局を活性化するために呼び出したとき、セルラー・ネットワークはあらかじめ計算されたディフィー・ヘルマンのデータ暗号化値から選択し、その値を直ちに移動局に対して送信することができる．

FIG. 1



【特許請求の範囲】

１．以降の送信のために複数のディフィー・ヘルマンのデータ暗号化値を作成するためのプロセスであって、

（ａ）前記データ暗号化値に対する要求を受信する前に一組のデータ暗号化値を生成し、前記データ暗号化値の組は公開モジュラスの値Ｎ、秘密のキーｙ、およびプリミティブ要素ｇから構成されるグループから少なくとも１つの値を含んでいるデータ暗号化値生成のステップと、

（ｂ）前記の一組のデータ暗号化値をデータベースの中に格納するステップとを含むプロセス。

２．請求項１に記載のプロセスにおいて、ステップ（ａ）およびステップ（ｂ）が繰り返し実行され、前記データ暗号化値の組の格納されたテーブルを前記データベースの中に作成するようになっているプロセス。

３．請求項１に記載のプロセスにおいて、

ステップ（ａ）は前記公開モジュラスＮ、前記秘密のキーｙおよび前記プリミティブ要素ｇに基づいて部分キーＹを計算するステップをさらに含み、

ステップ（ｂ）は、前記公開モジュラスＮ、前記プリミティブ要素ｇ、および前記部分キーＹを格納するステップを含むプロセス。

４．請求項２に記載のプロセスにおいて、前記データベースはセルラー・ネットワークの一部分であるプロセス。

５．請求項４に記載のプロセスにおいて、前記セルラー・ネットワークは移動局に対してデータを送信し、そして移動局からデータを受信し、そして前記プロセスが前記移動局の無線による活性化に

おいて使われるようになっているプロセス。

６．請求項４に記載のプロセスにおいて、前記セルラー・ネットワークは移動局に対してデータを送信し、移動局からデータを受信し、そして前記プロセスはさらに、

（ｃ）前記移動局の活性化のための要求を受信するステップと、

（ｄ）前記データベースから一組の現在のデータ暗号化値を選択するステップ

と、

（ｅ）前記セルラー・ネットワークからのデータ暗号化値の前記現在の組を前記移動局に対して送信するステップとをさらに含むプロセス。

７．請求項６に記載のプロセスにおいて、

ステップ（ｅ）において選択された前記データ暗号化値の現在の組に基づいて部分キーＹを生成するステップをさらに含み、

ステップ（ｅ）は、前記セルラー・ネットワークからの前記部分キーＹを前記移動局に対して送信するステップを含むプロセス。

８．請求項６に記載のプロセスにおいて、

（ｆ）前記現在のデータ暗号化値の組を前記移動局において前記セルラー・ネットワークから受信するステップと、

（ｇ）前記移動局において秘密の値ｘを生成するステップと、

（ｈ）前記移動局における前記秘密の値ｘに基づいて部分キーＸを生成するステップと、

（ｉ）前記移動局からの前記部分キーＸを前記セルラー・ネットワークに対して送信するステップとをさらに含むプロセス。

９．請求項８に記載のプロセスにおいて、

（ｊ）前記秘密のキーｘおよび前記データ暗号化値の現在の組に

基づいて前記移動局においてＡキーを生成するステップをさらに含むプロセス。

１０．請求項９に記載のプロセスにおいて、

（ｋ）前記部分キーＸを前記セルラー・ネットワークにおいて受信するステップと、

（ｌ）前記部分キーＸと前記データ暗号化値の現在の組に基づいて、前記セルラー・ネットワークにおいてＡキーを生成するステップとをさらに含むプロセス。

１１．請求項１０に記載のプロセスにおいて、

（ｍ）前記移動局における前記Ａキーを前記セルラー・ネットワークにおけるＡキーと比較するステップをさらに含むプロセス。

１２．請求項１０に記載のプロセスにおいて、前記移動局はメモリを含み、そして前記Ａキーは前記移動局の中の前記メモリの中および前記セルラー・ネットワークの中の前記データベースの中に、前記移動局の前記セルラー・ネットワークに対するそれ以降の認証のために格納されるようになっているプロセス。

１３．請求項８に記載のプロセスにおいて、前記データ暗号化値の現在の組が、前記移動局が前記セルラー・ネットワークに対して認証された後、前記データベースから消去されるようになっているプロセス。

１４．ディフィー・ヘルマンのデータ暗号化値をあらかじめ計算するための装置であって、

ソフトウェアの命令を実行し、ディフィー・ヘルマンのデータ暗号化値を、前記データ暗号化値に対する要求を受信する前に生成するプロセッサと、

前記ディフィー・ヘルマンのデータ暗号化値を格納するために前記プロセッサに対して結合されているデータベースとを含む装置。

１５．請求項１４に記載の装置において、Ａキーに基づいてデータを暗号化するために、前記プロセッサに結合されている符号化ブロックをさらに含む装置。

１６．請求項１４に記載の装置において、前記ディフィー・ヘルマンのデータ暗号化値を移動局に対して送信するために、前記マイクロプロセッサに対して結合されていて、無線周波段を備えている基地局をさらに含む装置。

【発明の詳細な説明】

改良形暗号化キーの生成

発明の分野

本発明は、データの暗号化技術に関し、特にセルラー・ネットワーク上の新しい移動局の活性化において使われるデータの暗号化の値を生成するためのプロセスに関する。

発明の背景

セルラー電話機またはセルラー・ネットワークに対して、移動局において新しいユーザを活性化するためのシステムが時によって使われてきた。その活性化のプロセスはセルラー・ネットワーク上に顧客の料金請求情報を格納し、そして移動局およびセルラー・ネットワークの両方において共有される秘密のデータを格納することを含む。その共有される秘密のデータはその移動局の電話番号、その製造者を識別するための情報およびその移動局のシリアル番号、およびその移動局とセルラー・ネットワークとの間で送信されるデータを暗号化するために使われる認証キー（Ａキー）を含む。暗号化されたデータは音声およびデータの両方を含むことができる。

移動局とセルラー・ネットワークにおいて共有される秘密のデータが存在することによって、その移動局のそれ以降において使われるセルラー・ネットワークに対する認証のために、高度化された双方向の検証技法を実装することができる。その双方向の検証技法は、セルラー・ネットワークに対して許可されていないアクセスを得て、許可されている加入者に対して料金が不正に請求されるようにする目的での、無線周波（ＲＦ）の盗聴の陰謀を制限するのに役立つ。

セルラー・ネットワークに対して移動局を活性化するためのよく知られている方法は、無線による活性化遠隔サービス（ｏｖｅｒ－ｔｈｅ－ａｉｒ ａｃｔｉｖａｔｉｏｎ ｔｅｌｅｓｅｒｖｉｃｅ）（ＯＡＴＳ）であり、米国電気通信工業会（Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎ Ｉｎｄｕｓｔｒｉｅｓ Ａｓｓｏｃｉａｔｉｏｎ）（ＴＩＡ）の標準ドキュメント番号：ＩＳ １３６の中で記述されている。ＯＡＴＳはディフィー・ヘルマン（Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ

）の方法として知られている、移動局とセルラー・ネットワークの両方においてＡキーを発生するための安全な方法を使用する。

ＯＡＴＳのプロセスは移動局にいるユーザからセルラー・ネットワークのための顧客サービス担当者に対しての電話呼出しから開始される。ユーザの呼出しに応答して、セルラー・ネットワークにおける認証センターがディフィー・ヘルマンの暗号化値を生成することを開始する。そのデータ暗号化の値は厳密な統計的条件のために、そのユーザが顧客サービス担当者と一緒に電話がつながっているままの状態で、生成するのに数分かかる。ディフィー・ヘルマンのデータ暗号化値の発生を待っていることはユーザにとって不便であり、新しいユーザを活性化するためのセルラー・ネットワークの能力を阻害する。

発明の概要

本発明は、以降の伝送のための複数のディフィー・ヘルマンのデータ暗号化値を生成するための方法を提供する。一組のデータ暗号化値が、そのデータ暗号化値に対する要求を受信する前に生成される。そのデータ暗号化値は、パブリック・モジュラス値Ｎ、秘密

キーＹおよびプリミティブ要素ｇから構成されるグループから少なくとも１つの値を含む。そのデータ暗号化値は次にデータベースの中に格納される。その生成および格納のステップを繰り返し実行して、データベースの中にデータ暗号化値の格納されたテーブルを作成することができる。

このプロセスは、無線による活性化を実装するためにセルラー・ネットワークにおいて使われる。新しいユーザが１つの移動局を活性化するために呼び出すと、セルラー・ネットワークは、既に利用可能なあらかじめ計算済みのディフィー・ヘルマンのデータ暗号化値の中から選択し、その値を移動局に対して直ちに送信することができる。このプロセスによって活性化のために必要な時間が大幅に削減され、したがって、新しいユーザおよびセルラー・ネットワークのプロバイダにおける負担が削減される。

図面の簡単な説明

これらおよび他の目的、特徴、および利点は以下の添付図面を参照することに

よって、より完全に理解される。

図１は、広く知られていて使われているセルラー・ネットワークの構成および移動局との対話のブロック図である。

図２は、移動局、基地局および認証センターの実施形態のブロック図である。

図３は、ＯＡＴＳのためのディフィー・ヘルマンの暗号化パラメータを生成する従来技術の方法のフローチャートである。

図４は、ＯＡＴＳに対するディフィー・ヘルマンの暗号化パラメータを独立に生成することを示している本発明の方法のフローチャートである。

発明の詳細な説明

図１は、広く知られていて使用されているセルラー・ネットワークの構成および、その移動局１０との対話のブロック図を示している。セルラー・ネットワーク１２は移動交換センター１４を備え、それは他の移動交換センター１４（図示せず）と結合することができ、そして１つまたはそれ以上の基地局１６に対しても結合され、そしてホーム・ロケーション・レジスタ１８、顧客サービス・センター２０、認証センター２２、公衆電話網（ＰＳＴＮ）２４および統合サービスディジタル通信網（ＩＳＤＮ）２６を備えている。

１つまたはそれ以上の移動局１０が基地局１６に対して信号を送信し、基地局１６から信号を受信することによって、セルラー・ネットワークと対話する。移動局１０が使用されているとき、それは現在の基地局１６（通常は、その移動局１０に最も近い基地局）に対して信号を送信し、その基地局から信号を受信する。移動局１０が現在の基地局１６から遠ざかるとき、現在の基地局１６は、その移動局１０をその移動局１０に最も近くなっている別の基地局１６に対して「ハンド・オフ」することができる。

移動交換センター１４は、移動局から発信され、そして移動局１０においてターミネートしている呼出しを、他の移動交換センター１４に対して、ＰＳＴＮ２４に対して、そしてＩＳＤＮ２６に対して切り換える。ホーム・ロケーション・レジスタ１８は移動局１０を識別し、そしてその移動局１０が現在存在している、あるいは普通に存在している地域の部分を示す。認証センター２２は、各移

動局１０とセルラー・ネットワーク１２との間で送信を暗号化する目的のために、各移動局１０に関連付けられているＡキー

を管理する。さらに、移動局１０の活性化時に、認証センター２２は、移動局１０に対する送信のためのデータ暗号化値を生成することができ、そしてそれ以降での送信に使われるためのＡキーを生成する目的のために、移動局１０から受信されたデータ暗号化値を処理する。

図２は、移動局１０、認証センター２２、およびセルラー・ネットワーク１２の基地局１６の略図を示し、新しい移動局１０の活性化を実行するために使われる実施形態を示している。移動局１０はメモリ３０に結合されているマイクロプロセッサ段２８、データの入力および出力（Ｉ／Ｏ）のソース３２、無線周波（ＲＦ）段３４および符号化ブロック３６を備えている。移動局１０におけるマイクロプロセッサ段２８は、他の機能ブロックと対話し、データを処理し、そして移動局１０を動作させるソフトウェア・プログラムの命令を実行する。また、移動局１０におけるマイクロプロセッサ段２８は、活性化およびデータ暗号化のプロセスにおいて使われる乱数およびデータ暗号化値も発生する。メモリ３０は、ランダム・アクセス・メモリ（ＲＡＭ）、読出し専用メモリ（ＲＯＭ）およびプログラム可能な読出し専用メモリ（ＰＲＯＭ）を含むことができる。ＲＯＭまたはＰＲＯＭは、その移動局の製造者およびシリアル番号を識別するための情報、その移動局の電話番号、およびその移動局のＡキーなどのその移動局に関するデータを永久的に格納するために使うことができる。データの入力および出力のソース３６によって、音声および他のデータを受信および送信すること以外に、ユーザは呼出しを掛け、その電話呼出しの伝送に関するメッセージを受信することができる。符号化ブロック３６はデータの暗号化を実行

する。無線周波段３４は移動局１０からデータを受信し、移動局１０に対して信号を送信する。

認証センター２２の単純化された実施形態も図２に示されている。また、セルラー・ネットワーク１２の基地局１６も無線周波段３７を備え、それは移動局１

０からデータを受信し、そして移動局１０へデータを送信する。基地局１６の無線周波数３７は認証センター２２に結合され、認証センター２２は、マイクロプロセッサ３８、メモリ４０、符号化ブロック４２、データベース４４、およびデータの入力および出力（Ｉ／Ｏ）のソース４６を含む。無線周波段３７は、認証センター２２に対して直接に接続されていなくてもよく、有線ネットワーク、別の無線周波段を通じて、別のセルラー・ネットワーク・コンポーネントを通じて、あるいはそれらの任意の組合せを通じて認証センター２２に対して結合することができる。

マイクロプロセッサ段３８は、認証センター２２が他の機能ブロックおよび移動局１０と対話し、そしてセルラー・ネットワーク１２によって要求されるように動作することができるようにするプログラム命令を実行し、そしてデータを処理する。認証センター２２にあるマイクロプロセッサ段３８は、セルラー・ネットワーク１２上で移動局の活性化のために必要なディフィー・ヘルマンのデータ暗号化値も生成することができる。メモリ４０は、マイクロプロセッサ３８によって必要とされるデータを格納するために使われる。符号化ブロック４２は、認証センター２２と移動局１０との間で送信されるデータを暗号化するために使われる。データベース４４は、加入者を認証して活性化するプロセスにおいて使われる情報、たとえば、１つまたはそれ以上の移動局１０の電話番号、移動

局１０の製造者およびシリアル番号を識別するための情報、および移動局１０に関連付けられているＡキーなどの情報を格納するためのデータベースである。また、データベース４４は、ディフィー・ヘルマンのデータ暗号化値のテーブルを格納するためにも使うことができ、その値は移動局１０をセルラー・ネットワーク１２に対して活性化する際に使われる。データの入力および出力のソース４６によって、認証センター２２はセルラー・ネットワーク１２の他の部分と対話することができ、そしてまた、認証センター２２の動作について人間の対話を行うこともできるようにする。

図３は、ディフィー・ヘルマンの方法を使っているセルラー・ネットワーク１２上での移動局１０の活性化のための従来技術の方法を示している。ステップ５

０において、認証センター２２は移動局１０からの活性化のための要求を待つ。要求が受信されると、認証センター２２のマイクロプロセッサ段２８が、ステップ５２においてディフィー・ヘルマンのデータ暗号化値の生成を開始する。

ディフィー・ヘルマンのデータ暗号化値の生成は、特定の、そして厳格な規則に従って行われるので時間が掛かる。広く使われている実施形態においては、認証センター２２は、秘密のキーｙおよび公開のモジュラスＮおよびプリミティブ要素ｇを生成しなければならない。

秘密のキーｙに対する統計的な必要条件は、それが次の統計的性質を持つ１６０ビットの乱数であることである。ｙは４より小さくてはならない；生成されるすべてのｙの値は、その統計的な分布がそれらの範囲にわたって一様でなければならない；生成されるすべてのｙは、同じまたは異なる移動局１０に対して生成される秘密

キーとは統計的に無相関でなければならない；異なる秘密キーに対して生成される数値は、以前に使用された数値および／または移動局の指示子の値から導くことができるようなものであってはならない；異なる認証センター２２によって生成される数値は、統計的に無相関でなければならない；そして認証センター２２は、その秘密キーｙをこの乱数の値に設定しなければならない。

公開モジュラスＮは、大きな素数でなければならない。公開モジュラスＮは、ＴＩＡ標準ＩＳ－１３６に規定されているように、少なくとも７６８ビットの素数であって最大が１０２４ビットであり、次の統計的性質を有している。Ｎは異なる移動局に対して異なっていなければならない；Ｎのすべての値の統計的分布はそれらの範囲にわたって一様でなければならない；Ｎのすべての値は同じか、あるいは異なる移動局１０に対するＮの他の値とは統計的に無相関でなければならない；Ｎに対する異なる値は任意の以前に使用された数値および／または移動局の指示子の値から導くことができるものであってはならない；異なる認証センター２２によって生成される数値は統計的に無相関でなければならない；（Ｎ－１）／２は大きな素数の因数を有していなければならない；そしてＮの最上位ビットは「１」に等しくなければならない。

公開モジュラスN、秘密のキーyおよびプリミティブ要素gを生成した後、マイクロプロセッサ３８は次に次の式に基づいて部分キーYを生成しなければならない。

$$Y = g^{y} \bmod N \qquad (式1)$$

次に、ステップ５４において、認証センター２２は公開モジュラスN、プリミティブ要素gおよび部分キーYを移動局１０に対して基

地局１６の無線周波段３７経由で送信する。

移動局１０は、N、g、およびYをステップ５６において受信し、そしてステップ５８において移動局１０は、マイクロプロセッサ段２８を使って乱数を発生し、その乱数が秘密のキーxとなる。次に、移動局１０はステップ６０において次の式を使って部分キーXを計算する。

$$X = g^{x} \bmod N \qquad (式2)$$

次に、移動局１０は、ステップ６２においてセルラー・ネットワーク１２に対して移動局１０の無線周波段経由でXの値を送信する。次に、ステップ６４においてセルラー・ネットワーク１２は部分キーXを受信する。ステップ６６において、移動局１０および認証センター２２は両方ともAキーを以下の式に基づいて計算する。

$$A\text{キー}_{MS} = (Y)^{x} \bmod N = (g^{y} \bmod N)^{x} = g^{yx} \bmod N \qquad (式3)$$

$$A\text{キー}_{AC} = (X)^{y} \bmod N = (g^{x} \bmod N)^{y} = g^{xy} \bmod N \qquad (式4)$$

次に、Aキーがセルラー・ネットワーク１２上および移動局１０上で格納され、セルラー・ネットワーク１２と移動局１０との間のそれ以降の送信における暗号化のベースとなる。

図４は、ディフィー・ヘルマンのデータ暗号化値の生成に関連する遅延をなくする本発明の方法を示している。移動局１０におけるユーザが活性化のためにセルラー・ネットワーク１２にコンタクトするのを待たずに、ステップ７０においてマイクロプロセッサ３８は、公開モジュラスN、プリミティブ要素g、および秘密のキーyを含んでいるディフィー・ヘルマンのデータ暗号化値を生成する。N、g、およびyが生成されると、それらはそれ以降の検索のために、ステップ

７２においてデータベース４４の中に格納される。次

に、データベース４４がステップ７４において一杯であった場合、あるいは認証センターによって決定されるいくつかの他の条件に達していた場合、ディフィー・ヘルマンのデータ暗号化値の生成が終了する。それ以外の場合、この方法がステップ７０から始まって繰り返され、その中で認証センター２２におけるマイクロプロセッサ３８がディフィー・ヘルマンのデータ暗号化値の別の組を生成する。ステップ７２においてこれらの値がデータベース４４に格納される。

このようにして、ディフィー・ヘルマンの利用可能な組のテーブルが、移動局１０において活性化時にユーザに対してそれ以降の送信のためにデータベース４４上に格納される。データ暗号化値のテーブルは認証センター２２における実装によって変化する可能性がある。N、g、y、およびYまたはそれらの１つまたはそれ以上の任意の組合せが有利である。本発明の１つの好適な実施形態において、格納された値のテーブルは以下のように示される。

N_1, g_1, Y_1

N_2, g_2, Y_2

N_3, g_3, Y_3

N_4, g_4, Y_4

ステップ７６において、認証センター２２はユーザからの活性化に対する要求を待つ。ステップ７６において活性化のための要求を受信すると、認証センター２２はステップ７８においてディフィー・ヘルマンのデータ暗号化値のデータベース４４から１つの値を選択する。ディフィー・ヘルマンのデータ暗号化値の組は先入れ先出し（ＦＩＦＯ）のベースで、あるいは任意の他の選択方式でデータベースからランダムに選択することができる。したがって、データ

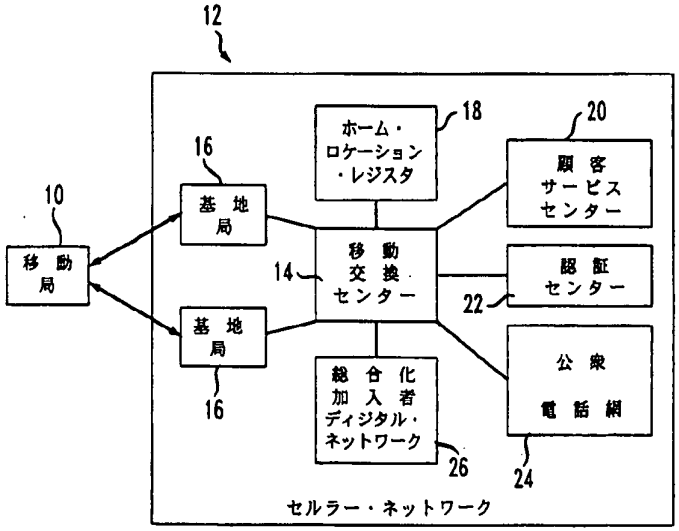
暗号化値は要求時に直ちに使える。次に、データベース４４の中に格納されているディフィー・ヘルマンの値に依存して、認証センター２２は追加の値を生成しておくことができる。N、g、およびYがデータベース４４の中に格納されていた場合、認証センター２２は追加の値を生成する必要はない。N、g、およびy

が格納されていた場合、認証センターは先ず最初にＹの値を上記の式１から生成しなければならない。Ｎ、ｇ、またはその両方が格納されていなかった場合、その欠落している値が生成されなければならない。Ｙまたはｙのいずれもが格納されていなかった場合、ｙが生成され、そしてそれから上記の式１に基づいてＹが生成されなければならない。ｙが格納されているが、Ｙが格納されいなかった場合、Ｙはその格納されているｙの値から上記の式１に基づいて生成されなければならない。次に、ステップ８０において、データ暗号化値Ｎ、ｇ、およびＹがＡキーの生成の一部として移動局に対して送信される。それ以降、図３に示されている方法のステップ５６～６６が実行されて活性化を達成することができる。

本発明の特定の実施形態が開示されてきたが、この分野の技術に熟達した人によって、それらの特定の実施形態に対して、本発明の精神および適用範囲から逸脱することなしに変更できることを理解されたい。

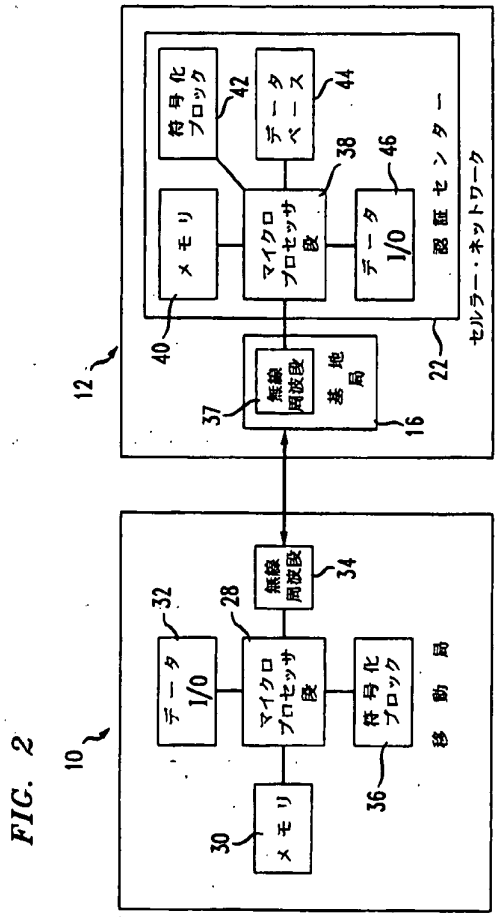
【図１】

FIG. 1



【図２】

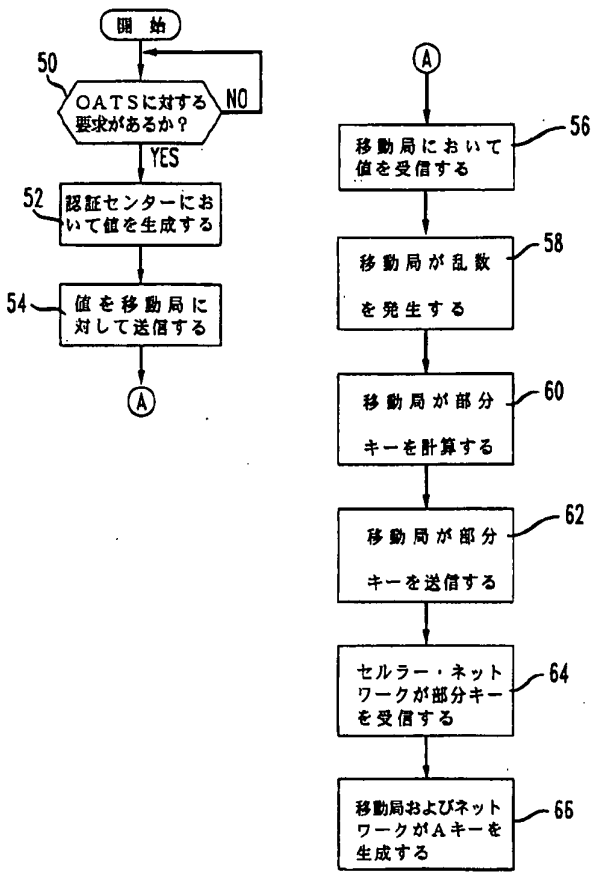
FIG. 2



【図3】

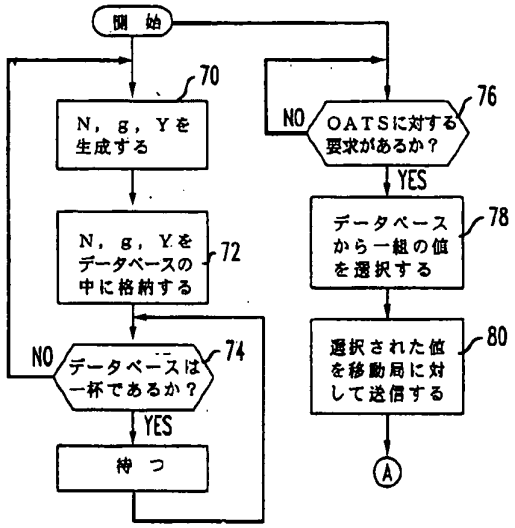
FIG. 3

従来技術



【図4】

FIG. 4



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No PCT/US 97/17585

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L H04C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	BELLER M J ET AL: "Batch Diffie-Hellman key agreement systems and their application to portable communications" ADVANCES IN CRYPTOLOGY - EUROCRYPT '92. WORKSHOP ON THE THEORY AND APPLICATIONS OF CRYPTOGRAPHIC TECHNIQUES. PROCEEDINGS, BALATONFURED, HUNGARY, 24-28 MAY 1992, ISBN 3-540-56413-6, 1993, BERLIN, GERMANY, SPRINGER-VERLAG, GERMANY, pages 208-220, XP002056427 see page 214, line 5 - page 215, line 1 ---- -/--	1,3-5

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents :
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 February 1998	10/03/1998
Name and mailing address of the ISA: European Patent Office, P.B. 5818 Patentlaan 2, NL - 2280 HV Rijswijk, Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Authorized officer: Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No PCT/US 97/17585

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	MATSUMOTO T ET AL: "On seeking smart public-key-distribution systems" TRANSACTIONS OF THE INSTITUTE OF ELECTRONICS AND COMMUNICATION ENGINEERS OF JAPAN, SECTION E (ENGLISH), FEB. 1986, JAPAN, vol. E69, no. 2, ISSN 0387-235X, pages 99-106, XP002056002	14
Y	see page 99, left-hand column, last paragraph - page 100, left-hand column, line 3; figure 1 ----	14-16
A	FRANKEL Y ET AL: "Security issues in a CDPD wireless network" IEEE PERSONAL COMMUNICATIONS, AUG. 1995, USA, vol. 2, no. 4, ISSN 1070-9916, pages 16-27, XP000517586	1,4,5
Y	see page 17, left-hand column, line 20 - line 43 ----	14-16
A	WO 96 28913 A (BELL COMMUNICATIONS RES) 19 September 1996 see page 13, line 11 - line 14 see page 16, line 7 - line 13 -----	1,14

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 97/17585

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9628913 A	19-09-96	US 5633928 A	27-05-97
		CA 2215050 A	19-09-96